UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE PREMISES LOCATED AT 629 LEE STREET
EDEN, NORTH CAROLINA 27288

Case No. 1:15MJ119

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The premises located at 629 Lee Street, Eden, North Carolina 27288 which is more particularly described in Attachment A, attached hereto.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the violations of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(5)(b), 2422(b), 1470, and 875(c), which are more particularly described in Attachment B, attached hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18USC§§2252A(a)(2),(a)(5)(b)	Receipt or Distribution of Child Pornography & Poss. of Child Pornography
18USC§2422(b)	Enticement of a Minor to engage in Sexual Activity
18USC§§1470 and 875(c)	Transfer of Obscene Matter to a Minor Under 16 & Threatening Communication

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Tara S. Cataldo, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: April 2, 2015

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT: 629 LEE STREET EDEN, NORTH CAROLINA 27288	Case No. 1:15 MJ 119

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Tara Cataldo, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 629 Lee Street, Eden, North Carolina 27288 (also referred to as "PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI), and have been since March of 2008. My initial training consisted of a twenty week FBI new agent course during which I received instruction on various aspects of federal investigations. In addition, I have received more than 350 hours of training related to computers and cyber matters, to include investigations of cyber crime. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency. Prior to joining the FBI, I worked in law enforcement for over eight years as a police officer and sheriff's investigator. I have been the case agent or

supporting agent in numerous investigations, including investigations involving child pornography, kidnapping, computer intrusion, and internet fraud.

3. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

4. I am investigating the activities of James Matthew Shelton (also referred to as "SHELTON"), who resides at the PREMISES. As will be shown below, there is probable cause to believe that SHELTON possesses child pornography and has received/distributed child pornography, enticed and attempted to entice a minor to engage in sexual activity, transmitted obscene material to a minor, and transmitted threats to injure the person of another in violation of 18 U.S.C. §§ 2252A(a)(5)(b), 2252A(a)(2), 2422(b), 1470, and 875(c).

5. The statements in this affidavit are based my knowledge and investigation into this matter, information and documents provided to me by FBI agents and task force officers and the Boyle County Sheriff's Office, and through a review of database records.

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of §§ 2252A(a)(5)(b), 2252A(a)(2), 2422(b), 1470, and 875(c) are presently located at the PREMISES.

PROBABLE CAUSE

7. On August 23, 2014, the mother of a minor male, born in January of 1999 and hereinafter referred to as "MG", reported to the Boyle County, Kentucky Sheriff's Office that MG and a second minor male, born in September of 1999 and hereinafter referred to as "ZB", both received a death threat from an adult male individual while on a four-way telephone call. MG and ZB referred to the adult male individual as "James" or "Matt".

8. MG was subsequently interviewed by a representative of the Boyle County Sheriff's Office and reported that the adult male individual had threatened to shoot and kill him and ZB during the phone call. MG further reported that ZB and a minor female, born in September of 1999 and hereinafter referred to as "NP", were both in possession of nude photographs of a second minor female, born in July of 2001 and hereinafter referred to as "KB". MG further reported that ZB had received these photographs from the adult male individual.

9. ZB, NP, and KB were subsequently interviewed and reported communicating with the adult male individual via Facebook and cell phone, including by text message. They identified the adult male individual's Facebook profile as james.shelton.773 and his cell phone number as 336-552-8945. All the minors reside and attend school in Kentucky.

10. Based on information provided by the minors, law enforcement representatives applied for and received a Commonwealth of Kentucky search warrant for the Facebook account james.shelton.773. On November 11, 2014, Facebook provided the information requested, including subscriber information, messages, and photos. I have reviewed the return from Facebook which reveals the following information about the user:

a. The user is listed as James Michael Shelton.

b. The user's cell phone number verified by Facebook for the account is 336-552-8945.

c. The date of birth listed on the profile is January 12, 1986.

d. The current city listed on the Facebook profile is Eden, North Carolina.

e. A "selfie" (a photograph taken of oneself using a cell phone and a mirror) contained within the Facebook messages depicts a tall male with glasses on.

11. A review of the Facebook return also revealed inappropriate conversations of a sexual nature between the user of the james.shelton.773 profile and the profile of NP. For example, on September 3, 2014 the james.shelton.773 profile sent NP the following message: "Ikr I'd Fuck u till ur legs quiver an jizz runs down ur inner thigh :-*" Further, it was revealed that, on August 25, 2014, the user of the james.shelton.773 profile sent NP six photographs of KB. Your affiant has reviewed these photographs. Four constitute child erotica. Two constitute child pornography and are described below:

a. A nude photograph of KB, age 13 at the time, with her thighs spread wide to display the genitalia.

b. A nude photograph of KB, age 13 at the time, with her thighs spread wide to display the genitalia and a sex toy inserted in the vagina.

12. Multiple administrative subpoenas were served on several different entities to identify the IP addresses associated with the Facebook profile james.shleton.773. Most of the responses to the subpoenas revealed that the IP addresses were associated with commercial locations or government offices in or around Rockingham County, NC. However, on November 25, 2014, Verizon Wireless responded to an administrative subpoena for the IP address 174.252.145.57 used by the Facebook profile james.shleton.773 on August 31, 2014. Verizon wireless provided information indicating that this IP address was assigned to Verizon's NAT router, meaning that the IP address was assigned to a cell phone. The cell phone utilizing that IP address on that specific date and time was revealed to be 336-552-8945.

13. The joint investigation between state and federal law enforcement agents identified the user of the Facebook profile james.shelton.773 and cell phone number 336-552-8945 as James Matthew Shelton, hereinafter "SHELTON", of 629 Lee Street, Eden, North Carolina 27288, hereinafter "PREMISES". On January 13, 2015, I verified through the North Carolina Department of Motor Vehicles (NCDMV) that SHELTON'S listed address is the PREMISES and that his listed date of birth is January 12, 1986. I viewed his North Carolina Identification Card photograph which was taken on or about March 10, 2014 and confirmed that the individual depicted appears to be the same individual depicted in "selfie" described above. I reviewed the Clear and Accurint databases which both list the PREMISES as SHELTON'S address and his phone number as 336-552-8945.

14. On September 10, 2014, a representative of the Boyle County Sheriff's Office interviewed KB. KB reported that she met SHELTON through NP. KB denied any in-person contact with SHELTON, but stated that she communicates with him via text message, phone, and

Facebook. KB informed SHELTON that she was 13 year old. SHELTON asked KB to have sex with him, but KB informed him that they would have to wait until she was 18 years of age. KB also reported that she sent nude photographs of herself to SHELTON and that he sent her nude photographs of himself. KB confirmed that SHELTON made threats to kill MG and ZB on the above described four-way call.

15. On March 18, 2015, KB was interviewed at a Child Advocacy Center in Kentucky. She admitted that she sent nude photographs of herself to SHELTON using her cell phone and said SHELTON sent her pictures of his penis using his cell phone number.

16. On September 10, 2014, a representative of the Boyle County Sheriff's Office interviewed ZB. ZB reported that SHELTON threatened to kill him and MG. ZB also admitted that SHELTON sent him nude photographs of KB via text message. Subsequently, ZB's cell phone was forensically analyzed. I conducted a review of the data contained on the phone and observed that SHELTON sent ZB six photographs of KB on August 25, 2014. These photographs were sent via MMS (multimedia message) to ZB's cell phone from the number 336-552-8945, SHELTON'S cell phone number. Two of these photographs constitute child pornography and are the same two images described above found via the Facebook search warrant.

17. The search warrant return from Facebook also revealed that SHELTON informed NP that he owns a shotgun which he keeps in the trunk of his car and that he plans to rob KB's family.

18. On March 10, 12, and 19, 2015, I and others conducted physical surveillance on the PREMISES. The dwelling located at the PREMISES is a one-story, cream-colored, wood-

sided home. On March 10, 2015, a person believed to be SHELTON was observed on the front porch using a cell phone. On March 19, 2015, a person believed to be SHELTON was seen in the backyard using a cell phone.

STATUTORY AUTHORITY

19. This investigation concerns alleged violations of 18 U.S.C. §§ 2252A(a)(5)(b), 2252A(a)(2), 2422(b), and 1470 which relate to the sexual exploitation of minors as well as 18 U.S.C. § 875(c) which relates to threatening communication.

a. 18 U.S.C. § 2252A(a)(5)(b) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that have traveled in interstate or foreign commerce.

b. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction was of such conduct.

c. 18 U.S.C. § 2422(b) prohibits knowingly persuading, inducing, enticing, or coercing any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or or attempting to do so.

d. 18 U.S.C. § 1470 prohibits using the mail, or any facility or means of interstate or foreign commerce, to knowingly transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempting to do so.

e. 18 U.S.C. § 875(c) prohibits transmitting in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.

DEFINITIONS

20. Based on my training and experience I use, I use the following technical terms to convey the following meanings in this Affidavit and Attachment B:

a. "Child Pornography" means any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

f. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

g. "Storage Medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

h. "IP Address" or Internet Protocol address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

"The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

"Peer-to-peer file-sharing," commonly known as"P2P," is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, conducting searches for files that are currently being shared on another user's computer and then downloading files from the other user's computer.

i. "Shared Folder" is a folder of files stored on a computer's local hard disk drive that can be used (or shared) by other users on the network or internet.

j. "Records" and "Information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

INFORMATION PERTAINING TO FACEBOOK

21. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users.

22. Facebook can be accessed by most computers that have the ability to connect to the Internet, including desktop computers, notebook computers, mobile phones, and tablets.

23. A Facebook user can also connect directly with other Facebook users by sending a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications and view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed", which highlights information about the user's "Friends", such as profile changes, photographs, and birthdas.

24. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

25. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on

Facebook, which also stores copies of messages sent by the recipient. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

26. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, electronic storage media, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

27. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

28. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

29. The ability to store images in digital form makes the computer and electronic storage media ideal repositories for child pornography. The size of hard drives used in home computers has

grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

30. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

31. Collectors and distributors of child pornography often use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

32. A continuing phenomenon on the Internet and frequent tool of individuals seeking child pornography is peer-to-peer file-sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible software. A user obtains files by opening the P2P software on the user's computer and conducting a search for files currently being shared on the network. P2P software often sets up its searches by keywords.

The results of a keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer sharing the file.

33. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one of file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often however, a user downloading a file receives the entire file from one computer.

34. Based on my training and experience, individuals who collect and engage in the exchange of child pornography tend to use multiple computers and/or storage medium to procure, distribute, and/or store child pornography. Further, cell phones, smartphones in particular, and tablets have the capability to be backed up onto other computers, often desktop computers and notebook computers. This can be accomplished by simply connecting the two devices by means of a USB cord. Further, "cloud" storage is becoming an increasingly popular means to store electronic records. Individuals are able to upload records to a remote server or a "cloud" and then access and download these records from any computer with the ability to connect to the Internet. As is the case with the majority of individuals engaged in today's hi-tech society, individuals who are interested in child pornography do not limit their activities to one computer or electronic storage device and take advantage of the way that multiple computers and electronic storage devices can be interconnected and used in concert.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

35. As described in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are

overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of

a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search

warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the

offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence

or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

40. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Tara Cataldo
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 2nd day of April, 2015.

L. Patrick Auld
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCIRPTION OF PREMISES TO BE SEARCHED

The premises located at 629 Lee Street, Eden, North Carolina 27288, including the residential dwelling, any out buildings such as a detached garage, shed, or barn, and any vehicle located on the premises. The dwelling located on the premises is pictured below. The numbers "629" are located on the front of the dwelling. The premises is listed in Rockingham County Deed Book 725 page 838 as Parcel Number 105352 and Long PIN number 707011568637. The premises is designated by the blue rectangle in the aerial photograph below.

ATTACHMENT B

PROPERTY TO BE SEIZED

1. All records relating to violations of 18 U.S.C. §§ 2252A(a)(5)(b), 2252A(a)(2), 2422(b), 1470, and 875(c) as follows:

   a. records and information constituting and referencing child pornography, as defined in 18 U.S.C. 2256(2)(A);

   b. records and information constituting and referencing "child erotica".

   c. records and information constituting and referencing any communication to or from NP, KB, MG, and ZB, to include solicitation to engage in any sexual activity;

   d. records and information constituting and referencing communication with any unidentified minors soliciting or referencing sexual activity or engaging in grooming behavior;

   e. records and information constituting and referencing images of male genitalia, including images of SHELTON'S penis distributed to minors;

   f. records and information referencing the Facebook profile james.shelton.773, including those indicating the owner and user thereof;

   g. records and information revealing and referencing IP addresses associated with the Facebook profile james.shelton.773;

   h. records and information referencing the cell phone number 336-552-8945;

   i. records and information constituting and referencing malicious software;

   j. records and information constituting and referencing threats to injure to ZB and MG to include records and information concerning the ownership of firearms and ammunition.

k. records and information revealing and referencing the ownership, occupancy, or possession of the searched premises.

2. Computers and storage media capable of containing the described above in paragraph one.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Any firearms, ammunition, and firearm magazines.

5. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

g. evidence of the times the COMPUTER was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

j. records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "Storage Medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.